

Datenschutz TIPPS

für Eltern

Kinder- und Jugendtelefon
0800-1110 333
nummergegenkummer.de



▶ So sind persönliche
Daten im Internet sicher

klicksafe.de

Mehr Sicherheit im Internet
durch Medienkompetenz

Datenschutz TIPPS

für Eltern

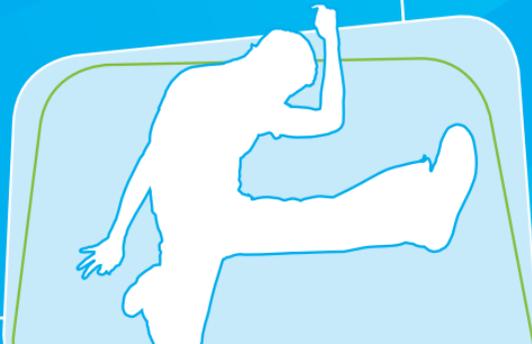
Liebe Eltern!

Viele Kinder und Jugendliche glauben, Datenschutz sei langweilig und gehe sie nichts an. Überzeugen Sie Ihr Kind vom Gegenteil!

Denn jeder Internet-Nutzer hinterlässt Spuren im Netz. Manche Daten verraten die Nutzer freiwillig. Häufig merkt man aber auch gar nicht, dass persönliche Daten im Hintergrund gesammelt werden. Zum Beispiel greifen viele **Apps** (Spiele oder kleine Programme in Sozialen Netzwerken oder auf dem Handy) während der Nutzung auf persönliche Kontakte, das Telefonbuch oder andere Daten zu. Über mobile Geräte wird immer häufiger auch der aktuelle Aufenthaltsort im Internet veröffentlicht.

Der vorliegende Flyer will Ihnen dabei helfen, persönliche Daten im Internet bestmöglich zu schützen und das Thema „Datenschutz“ mit Ihren Kindern zu besprechen.

Ihr klicksafe-Team



1

Datenschutz macht Sinn

► Persönliche Daten, zum Beispiel Adresse, Alter, Telefonnummer oder Interessen, nennt man auch „**personenbezogene Daten**“. Sie verraten viel über die eigene Person, sind kostbar und bedeuten für Unternehmen bares Geld. Und sie können von anderen missbraucht werden. Schützt man seine Daten, heißt das Privatsphäre, Anonymität und mehr Sicherheit im Internet! Dies sollte auch jüngeren Internet-Nutzern klar sein!

Das heißt aber nicht, dass Ihr Kind ganz auf persönliche Informationen im Netz verzichten muss. Entscheidend ist die richtige Auswahl. Hier können Ihrem Kind die folgenden **Tipps** helfen:

- Denk an das lange Gedächtnis des Internets: Dinge, die Du heute ins Netz stellst, gefallen Dir in ein paar Jahren vielleicht überhaupt nicht mehr. Aber im Internet stehen sie dann immer noch.
- Überlege **vor** dem Hochladen: Wie willst Du Dich im Internet (im schlimmsten Fall) für immer zeigen? Auch die „Oma-Regel“ kann Dir bei der Entscheidung helfen, nach dem Motto: Was würde meine Oma dazu sagen? Oder: Würde ich dies meiner Oma sagen oder zeigen?

- 🌐 Die schöne neue Welt der Überwachung: www.panopti.com.onreact.com
- 🌐 Tipps zum Datenschutz in mobilen Netzen finden Sie unter www.handysektor.de.

2

Datenschutz ist ihr gutes Recht

► Durch das „**Recht auf informationelle Selbstbestimmung**“ sind persönliche Daten (Name, Adresse, ...) in Deutschland sogar per Gesetz vor unerlaubter Verwendung geschützt. Das bedeutet: Niemand darf diese Daten ohne Einwilligung der betroffenen Person speichern, veröffentlichen oder weitergeben. Ausnahmen gibt es für einige staatliche Einrichtungen, wie zum Beispiel Meldeämter oder die Polizei.

Bei Fotos und Filmen gilt das „**Recht am eigenen Bild**“: Ausschließlich die abgebildete Person darf entscheiden, welche Bilder von ihr (z. B. in einem Sozialen Netzwerk) veröffentlicht werden. Ausnahmen gelten für Bilder, auf denen man Teil einer Menschenmenge oder nur „Beiwerk“ ist (Beispiel: Jemand fotografiert den Reichstag und Sie oder Ihr Kind stehen zufällig daneben).

Übrigens: Ist Ihr Kind jünger als 12 Jahre alt, haben rechtlich gesehen ausschließlich die Eltern/Erziehungsberechtigten bei Veröffentlichungen zu entscheiden. Zwischen 12 und 18 Jahren hängt es nach Meinung vieler Juristen vom Entwicklungsstand und der damit verbundenen Einsichtsfähigkeit des Kindes ab, ob es eigenverantwortlich über Bildveröffentlichungen entscheiden darf. **Tipp:** Tauschen Sie sich regelmäßig mit Ihren (jüngeren) Kindern über veröffentlichte Fotos aus und bleiben Sie in Sachen „Datenschutz“ im Gespräch.

- ⊕ Checked4you – Deine Rechte im Web (Klicken Sie auf „Computer + Internet“, dann auf „Internet“): www.checked4you.de



3

Jeder hat ein Recht auf Datenschutz

► Ihr Kind sollte nicht nur die eigenen, sondern auch die Persönlichkeitsrechte anderer beachten. Denn: Jeder hat ein Recht am eigenen Wort und am eigenen Bild. Machen Sie Ihrem Kind klar, dass es ohne deren Erlaubnis keine Bilder, Filme und Infos (wie z. B. den aktuellen Aufenthaltsort) von anderen ins Netz stellt. Absolut verboten ist es, falsche Daten über jemanden zu veröffentlichen. Das wäre Rufschädigung und kann strafbar sein.

Tipp für ihr Kind: Denk nicht nur an Dich, beachte auch die Rechte anderer! Also keine Bilder, Filme oder private Infos von Freunden, Bekannten oder anderen Personen ins Netz stellen – außer Du hast ihre Erlaubnis.

- ⊕ Unter www.irights.info finden Sie weitere Infos zum Thema „Urheberrecht in der digitalen Welt“.
- ⊕ Auf www.chatiquette.de werden Tipps und Benimmregeln fürs Chatten vorgestellt.

4

So wird ihr Kind ein Datenprofi in Sozialen Netzwerken

► Für den Schutz der eigenen Privatsphäre ist Ihr Kind auch selbst verantwortlich. Es sollte darauf achten, wie es sich im Internet zeigt! Geben Sie Ihrem Kind die folgenden **Tipps** mit auf den Weg:

- Ein Foto darf ruhig auch mal lustig sein. Allzu **peinliche** oder **beleidigende** Fotos oder Meinungen haben in Sozialen Netzwerken aber nichts zu suchen. Sie können auch Jahre später wieder im Netz auftauchen und Dich sogar den Ausbildungsplatz kosten.
- Überlege auch, was eine **Gruppenmitgliedschaft** über Dich aussagt. Die Gruppe „Saufen bis der Arzt kommt“ ist keine gute Werbung für Dich. Hassgruppen, in denen andere gezielt beleidigt werden, gehen gar nicht.
- Sei sorgsam mit Deinen **Profil-Daten**: Lass Anschrift, Telefon- oder ICQ-Nummern (ICQ ist ein Programm zum Nachrichtenaustausch in Echtzeit) weg. Sie sind nicht nötig, wenn du Dich mit anderen austauschst. Auch Deine private E-Mail-Adresse solltest Du nicht jedem geben.
- Überprüfe regelmäßig Deine **Privatsphäre-Einstellungen**. Hier helfen Dir die klicksafe-Leitfäden (siehe rechts).
- Prüfe genau, wem Du freien Zugang zu Deinen **privaten** Fotos und Daten gibst. Du weißt nie, was andere mit den Informationen machen!

Wenn Ihr Kind ein Soziales Netzwerk nicht mehr nutzen will, dann sollte es seine Mitgliedschaft beenden und die Profildaten löschen. So wird das Auffinden persönlicher Daten zumindest erschwert.

- ⊕ Die „Leitfäden für die Kommunikation im Netz“ zeigen Schritt für Schritt, wie man Daten in Sozialen Netzwerken schützen kann: www.klicksafe.de/materialien.
- ⊕ Zum persönlichen Schutz kann Ihr Kind auch das eigene Profilfoto witzig verändern: www.netzcheckers.de. (Klicken Sie auf „Workshops“, dann auf „Profilbilder und Icons“).
- ⊕ Flyer „Big brother is watching you!“ – Download unter: www.jugendinfo.de/pass-auf-dich-auf.

5

Das Internet vergisst nicht

► Reden Sie mit Ihrem Kind darüber, dass im Internet veröffentlichte Infos, Filme oder Fotos ab da nicht mehr privat sind. Einmal im Internet, beginnen diese Daten ein **Eigenleben**. Sie verbreiten sich, gelangen in Suchmaschinen und Online-Archive. Sie werden von anderen kopiert und weitergereicht. Dies alles wieder rückgängig zu machen, ist nahezu unmöglich. **Tipp**: Vor dem Hochladen überlegen, was wirklich alle von einem wissen sollen!

- ⊕ Das Internet-Archiv „WayBack Machine“ speichert Webseiten als Zeitdokumente dauerhaft ab: www.archive.org.
- ⊕ Videos „Think Before You Post“: www.smiley-ev.de/think_before_you_post.php
- ⊕ Videos auf www.klicksafe.de/spots

6 Elektronische Datenspuren hinterlässt man unbemerkt

- ▶ Technische Daten werden automatisch übertragen, ohne dass man es merkt. Gerade dies ist Kindern und Jugendlichen häufig nicht klar. Zwei Beispiele:
- Jeder Computer im Internet hat eine **IP-Nummer**. Das ist eine Art „Telefonnummer für das Internet“. Damit erkennen Experten, wann, wie lange und auf welchen Seiten der Nutzer im Netz unterwegs war. Über diese Nummer werden zum Beispiel illegale Musikdownloads ermittelt.
- Das Kind besucht die Seite seiner Lieblingsband und sieht kurze Zeit später auf einer anderen Seite eine Werbung für ihre neue CD. Schuld daran können **Cookies** (wörtlich „Kekse“) sein. Cookies sind kleine Dateien, die auf dem Computer gespeichert werden. Sie „merken“ sich genau, welche Seiten besucht worden sind. So können Unternehmen den Internet-Surfer beobachten und herausfinden, welche Interessen er hat.

🌐 Mehr Informationen zum Thema „Cookies“ finden Sie auf www.klicksafe.de (Suchbegriffe: Cookies Spyware).

7 Nicknames nutzen – unerkant surfen

- ▶ Ein guter **Nickname** („Deckname“) kann dabei helfen, im Internet unerkant zu surfen. Hierbei ist Erfindungsgeist gefragt. Ein Deckname der dem richtigen Namen zu ähnlich ist oder das Alter enthält, hilft wenig. Ihr Kind kann ihn zum Beispiel in Blogs, Chats und Foren benutzen. Machen Sie Ihrem Kind auch klar, dass es sich nicht hinter einem Nick verstecken oder sich als jemand anderer ausgeben soll, um andere gezielt zu beleidigen. Das ist unfair und kann sogar bestraft werden!
- ! Je häufiger Ihr Kind im Internet unterwegs ist, umso sicherer ist es, wenn es verschiedene Nicks verwendet. So haben Beleidigungen, Betrug und anderer Datenmissbrauch eine geringere Chance.



8

So behält ihr Kind die Kontrolle über seine Daten

► Je mehr persönliche Daten Ihr Kind im Internet veröffentlicht, umso weniger können diese kontrolliert werden. **Datensparsamkeit** lohnt sich und schützt vor bösen Überraschungen. Gemeinsam mit Ihrem (jüngeren) Kind können Sie entscheiden, welche persönlichen Daten es ohne Probleme im Netz veröffentlichen darf. Fragen Sie Ihr Kind, ob es seine Daten (noch) im Griff hat!

Häufig veröffentlichen aber auch andere Personen private Dateien, Informationen oder Fotos von Ihrem Kind. Aus diesem Grunde sollte der eigene „**Online-Ruf**“ regelmäßig in verschiedenen Suchmaschinen geprüft werden. In Sozialen Netzwerken sollte man Profile und Fotoalben von Freunden nach Inhalten, die die eigene Person betreffen, prüfen und ggf. um Entfernung bitten.

⊕ Personensuchmaschinen: www.yasni.de, www.123people.de

9

Die AGBs – Was der Anbieter mit den Nutzerdaten machen darf

► Gerade Kindern und Jugendlichen fällt es häufig schwer, die **AGB**, die Allgemeinen Geschäftsbedingungen eines Internet-Angebots, zu lesen und zu verstehen. Vor allem die hier enthaltene **Datenschutzerklärung** ist überaus wichtig und sollte genau studiert werden. Der Nutzer erfährt dort, was mit seinen Daten passiert, was gespeichert, weitergegeben oder für Werbung genutzt wird. Und mit einer Anmeldung stimmt man den AGB automatisch zu! **Tipp:** Vereinbaren Sie mit Ihrem Kind, dass Sie neue Internet-Angebote vor einer Neuansmeldung gemeinsam anschauen und prüfen. Sagen Sie Ihrem Kind, dass es sich bei Fragen jederzeit an Sie wenden kann. Im Zweifel sollte Ihr Kind lieber auf eine Anmeldung verzichten – auch wenn es häufig schwerfällt.

Hier **zwei Beispiele** von vielen:

- Vielen **Apps** (kurz für Applications, also Programme) gibt man allein durch die Nutzung sämtliche Rechte an allen versendeten Inhalten ab. Damit darf der Anbieter des Programms beispielsweise auch an Freunde verschickte Nachrichten speichern, bearbeiten und sogar veröffentlichen.
- Viele kostenlose **E-Mail-Anbieter** „lesen“ die Inhalte von E-Mails automatisch nach Schlüsselwörtern aus, um dem Nutzer dazu passende Werbung zu senden.

⊕ Auf www.watchyourweb.de finden sich unter „Unsere Themen – Handysicherheit“ auch Infos zu Handy-Apps und Datenschutz.

10

Andere machen sich ein genaues Bild von ihrem Kind

► Unternehmen wollen möglichst viel von Ihren Nutzern erfahren. Sie haben ein Interesse daran, die Klicks und Angaben, die man auf verschiedenen Seiten gemacht hat, zu verknüpfen. Alle Daten, die sich über eine Person im Internet finden lassen, können zu einem **Nutzerprofil** zusammengestellt werden. So können Unternehmen passende Werbung zeigen, oder die Nutzer mit Werbemails zuschütten. Denn je mehr man von einem Nutzer weiß, desto eher kann man ihn zielgenau umwerben. Diese **personalisierte Werbung** ist häufig so geschickt, dass man gar nicht merkt, wie man zum Kauf bestimmter Produkte überzeugt werden soll.

- 🌐 Infos und Tipps zum Thema „Datenschutz im Internet“: www.datenparty.de
- 🌐 Mehr Infos zum Thema „Werbung“ gibt es auf www.klicksafe.de. (Klicken Sie auf „Themen“, dann unten links auf „Werbung“).

11

Tipps: Richtig reagieren bei Datenmissbrauch

► Sollten Sie oder Ihr Kind im Internet unerwünschte persönliche Daten, Infos oder Bilder finden, dann gehen Sie gemeinsam mit Ihrem Kind dagegen vor. Sagen Sie Ihrem Kind auch, dass es sich bei solchen Problemen immer an Sie wenden kann.

- Wenn Sie wissen, wer die problematischen Infos oder Bilder im Internet veröffentlicht hat, sollten Sie zunächst diese Person bitten, die Inhalte so schnell wie möglich zu löschen. Geben Sie hier eine konkrete Frist an, bis zu der die Inhalte entfernt sein müssen.
 - Wenn dies nichts bringt, informieren Sie den Betreiber der Seite und bitten um Löschung (Sie finden die Kontaktdaten im **Impressum** der Internetseite – gesetzlich vorgeschriebene Angabe über den Verantwortlichen für die Internetseite – oder über www.whois.net und www.denic.de). In Sozialen Netzwerken gibt es hier spezielle Melde-Buttons.
 - Die „**Datenschutz-Aufsichtsbehörden der Länder**“ (siehe unten) können Ihnen bei Datenschutzverletzungen ebenfalls mit Rat und Tat zur Seite stehen.
 - In schlimmen Fällen (schwere Beleidigungen, sehr problematische Bilder, die schnell entfernt werden sollen) sollten Sie auch die Polizei einschalten.
 - Bei verbotenen oder jugendgefährdenden Inhalten (z. B. pornografische Bilder) helfen Ihnen die **Beschwerdestellen** www.jugendschutz.net oder www.internet-beschwerdestelle.de.
- 🌐 Die Adressen der Datenschutz-Aufsichtsbehörden finden Sie auf www.bfdi.bund.de. (Klicken Sie auf „Datenschutz – Anschriften und Links“ dann auf „Aufsichtsbehörden für den nicht-öffentlichen Bereich“).
 - 🌐 Virtuelles Datenschutzbüro: www.datenschutz.de

12

Sicherheitstipps – So sind die Daten Ihrer Familie gesichert

- Benutzen Sie **sichere Passwörter** (mindestens achtstellig, Mischung aus Groß- und Kleinschreibung, Ziffern und Sonderzeichen) und nicht immer das gleiche. Ein Passwort sollte nicht leicht zu erraten sein (also nicht der Name eines Haustieres, ein Spitzname oder ähnliche leicht zu erschließende Wörter). Merksätze können dabei helfen, die Passwörter nicht zu vergessen.
- Erklären Sie Ihrem Kind, warum es Passwörter nicht weitergeben sollte. So wird verhindert, dass Fremde auf wichtige Daten zugreifen können.
- Installieren Sie ein **Anti-Virenprogramm** und aktualisieren Sie es regelmäßig.
- Schützen Sie Ihren Computer mit einer **Firewall** („Brandwand“). Eine Firewall schützt vor Angriffen und unberechtigten Zugriffen aus dem Internet und sollte nie ausgeschaltet werden.
- Sichern Sie Ihr **WLAN-Netzwerk** über eine verschlüsselte Verbindung (möglichst WPA2). Von unterwegs sollte man beim kabellosen Surfen keine wichtigen Daten verschicken.
- Schalten Sie WLAN und Bluetooth aus, wenn es nicht benötigt wird.
- Führen Sie regelmäßig **Sicherheitsupdates** (Update=Aktualisierung) Ihres Betriebssystems durch. Am besten stellen Sie es so ein, dass Sie wichtige Updates automatisch erhalten. So werden Sicherheitslücken geschlossen.

- Sagen Sie Ihrem Kind, dass es keine E-Mails mit **unbekanntem** Absender öffnen sollte, vor allem keine mitgeschickten Dateien.
 - Auch sollte es nicht auf unerwünschte E-Mails antworten. Weitere nervige Mails wären die Folge! Am besten legen Sie jedem Familienmitglied **zwei verschiedene E-Mail-Adressen** an. Eine sollte nur an gute Freunde und Bekannte weitergegeben werden. Die andere verwendet man für Anmeldungen, Online-Shopping und so weiter.
- 🌐 **www.klicksafe.de:** Unter „Themen – Datenschutz“ finden Sie weitere Infos und ein spannendes Quiz zu diesem Flyer, welches Sie gemeinsam mit Ihren Kindern spielen können (siehe unten). Das Quiz kann auch ein guter Aufhänger sein, um über das Thema „Datenschutz“ ins Gespräch zu kommen.



Bist Du ein Datenprofi im Internet?

Das Quiz zum Flyer "Datenschutz-Tipps für Jugendliche"

Gib Deinen Namen ein.

Weiter

Bist Du ein Datenprofi im Internet?

Mach das Quiz unter
www.klicksafe.de/quiz

▷ klicksafe (www.klicksafe.de) ist eine Initiative im Safer Internet Programme der Europäischen Union für mehr Sicherheit im Internet. klicksafe wird gemeinsam von der Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz (Koordination) und der Landesanstalt für Medien Nordrhein-Westfalen (LfM) umgesetzt.

Es wird darauf hingewiesen, dass alle Angaben in diesen Tipps trotz sorgfältiger Bearbeitung ohne Gewähr erfolgen und eine Haftung der AutorInnen ausgeschlossen ist.



Unveränderte nichtkommerzielle Vervielfältigung und Verbreitung ist ausdrücklich erlaubt unter Angabe der Quelle klicksafe und der Webseite www.klicksafe.de.

Siehe: <http://creativecommons.org/licenses/by-nc-nd/3.0/de/>

Coverfoto: © WavebreakMediaMicro - www.fotolia.com

Herausgeber:

klicksafe

c/o Landesanstalt für Medien

Nordrhein-Westfalen (LfM)

Zollhof 2

D-40221 Düsseldorf

T: +49 (0)211-77 00 7- 0

F: +49 (0)211-72 71 70

E: klicksafe@lfm-nrw.de

W: www.klicksafe.de

klicksafe wird gefördert von der Europäischen Union

- Vollständig aktualisierte Auflage 2012 -

